CRYPTER & DECRYPTER VOS MESSAGES AVEC PGP

(MAC OS X)



AU NOM D'ALLAH LE TOUT MISÉRICORDIEUX, LE TRES MISERICORDIEUX

L'équipe ***du Centre Médiatique An-Nûr*** *a le plaisir de vous présenter son document sur le cryptage de Message / Mail via PGP.*



Nous allons maintenant voir comment envoyer et recevoir des messages via le **cryptage PGP** qui, de nos jours, reste un des meilleurs moyens de faire passer un message ou encore un Email de façon sécurisée. Ce système de cryptage (avec un bon mot de passe choisi auparavant) est impossible à craquer. Actuellement, les gouvernements se cassent la tête sur les cryptages avec une **clef 2048 bits** donc, de ce fait, nous allons voir comment crypter son message avec une **clef 4096 bits**.

1 – INSTALLATION DE GPG SUITE POUR MAC :

Cette étape est relativement très simple. Allez sur le site internet https://gpgtools.org/ et téléchargez *GPG Suite* pour **OSX**. Une fois téléchargé, cliquez sur le fichier **.dmg** et sélectionnez ensuite « *Install* ».



Cliquez sur suivant jusqu'à ce que le logiciel s'installe entièrement. Ensuite, une fenêtre nommée « *GPG Keychain* » apparaît et vous propose de configurer votre première clef de chiffrement. Remplissez toutes les cases, « *Nom et prénom* », « *Courriel* » (pour voir quel mail sera utilisé pour vos messages cryptés, sélectionnez « *Options avancées* » et changez le « *Type de clé* » à **4096 bits**. Choisissez une phrase secrète qui servira pour **Crypter/Decrypter** vos mails.

Afin de préserver un maximum vos messages, il est préférable de choisir des longs mots contenant des caractères spéciaux, par exemple : *fzef799@fze)(gre@.*

Patientez maintenant que le processus prépare comme il faut votre clef de cryptage. Une fois terminé, elle apparaitra dans votre liste.

Nous allons maintenant voir comment rajouter un raccourci très utile pour Crypter et un autre pour Décrypter vos messages en toute simplicité sur votre mac. Allez dans « *Préférence système* » de votre ordinateur, puis dans « *clavier* », « *raccourcis* ». Allez dans « *Services* » sur la gauche, et dans le menu « *Texte* » vous voyez maintenant plusieurs options de raccourcis disponibles d'**OpenPGP**. Cochez « *OpenPGP : Encrypt Selection* » qui est par défaut *Cmd* + *Shift* + *E*, et aussi « *OpenPGP : Decrypt Selection* » qui est par défaut *Cmd* + *Shift* + *D*. Les lettres sont liées à l'action, donc très facile à retenir.

2 – CRYPTAGE ET DECRYPTAGE DES MESSAGES :

a) Envoyer un message crypté :

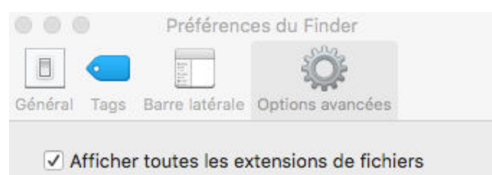
À ce stade-là, la personne avec laquelle vous souhaitez échanger vos messages cryptés doit vous faire parvenir sa **clef publique**, qui servira à crypter votre message pour qu'elle puisse par la suite le décrypter avec sa **clef privée** et son mot de passe.

Prenons donc l'exemple tout simple d'une **clef publique** (nous avons inventé le code, il n'est en aucun cas réel) :


```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: GPGTools - https://gpgtools.org

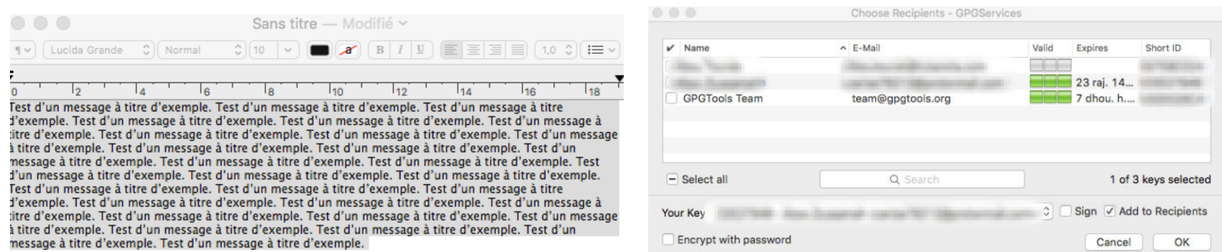
mQINBFcmIVkBEACeONtIKYPKQRIEXRCg6eOf7vFjcAisgimc1OLFuhnWZ+OtqO+0
Y3bgEgdOcgDR/2dIyUCZ6pUKxRwlym5sBabouUOyZQardPomKtQrIoYeCujn5Pcj
FTKlKIVVBq/QCWQl4VwyKzgRXFQPI5wbe02e5PYrtFrtf6oAGrmJQCUkwyCOHIdi
xoTEF/7SoSWja3so31M61N1WZJxGj1VS6JYBB8rtInW34gqigpu//K98PNGtzFnd
8uLNusfpa8D002n2YzWvsfEKr8069VxIkVbYsvDLor5G9PlPqEkidcEAqW6lnkjV
ybNOBSpNVVAVaZuNkLR6oPGxL1E3eWAJHUCYv4uyuh2yFSYlBrJ5HQUz2nfBV6DZ
vGqU5973ykuoMnXTPv/H1OYDWcblMx0HPDmZFHL25DrbqoksHylV6Fpi/Ga/fH6A
HwNfm9Sldb172FLBy6Is0y+zAjzPKCTn3i8m5Vl1oT6/92FSprPJWSSUA5wuxS8B
gOMya+U2myS+mnCL3dmq0LNvXqFpnobEfLCvYx8UvGt2pVYCY1FInWflsnt/KAhL
l/X6AfKVini9sWVvvf8rEddVSuSxrfmiKlyWDnM/89VORM/w91n8HS1/rrIXxF6a
UcSLQ0Cmjv79s6+wy6lAdokc9kvkSiQ6m8tl94w+woJBHW6rgN4sdUt78wARAQAB
tCpBYm91IE91c3NhbWFoIDxjZXJpc2U3NjIxM0Bwcm90b25tYWlsLmNvbT6JAj0E
EwEKACcFAlcmIVkCGwMFCQdMHYAFCwkIBwMFFQoJCAsFFgIDAQACHgECF4AACgkQ
Ree4Ks7ieUaCJhAAgEiTqZfsUl5M4J/kdRrddTCmQbMadOE3sg/I6EobEfLCvYfD
=l7hO
-----END PGP PUBLIC KEY BLOCK-----
```


Vous devez par la suite la coller dans l'éditeur de texte, **TextEdit.app**, et enregistrer le fichier. Ensuite, allez à l'endroit où vous avez enregistré ce fichier texte et renommez l'extension du fichier en *.asc*. Par défaut, il est soit en *.txt* soit en *.rtf*, ensuite vous pouvez double cliquer dessus et ça vous importe la **clef publique** de la personne dans la fenêtre « *GPG Keychain* ». Si vous ne voyez pas l'extension de vos fichiers, vous pouvez activer l'option en allant dans les préférences du *Finder*, « *Options avancées* » et cochez « *Afficher toutes les extensions de fichiers* ».

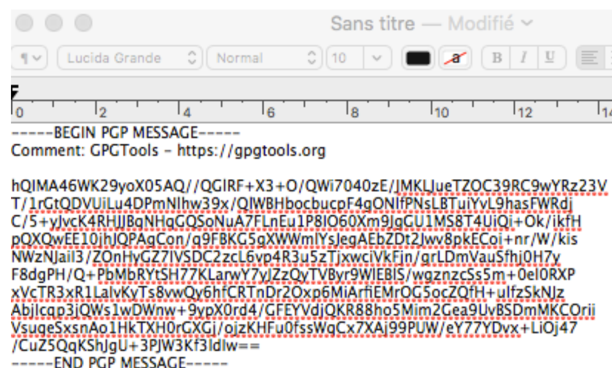


Une fois la clef publique de la personne importée dans votre liste, vous pouvez écrire un message dont vous souhaitez crypter. Sélectionnez-le entièrement et cliquez sur les touches préalablement configurées *Cmd* + *Shift* + *E*, pour crypter le

message. Une fenêtre s'ouvre et il vous sera demandé de sélectionner la **clef** avec laquelle vous souhaitez crypter le contenu. Sélectionnez alors celle de la personne voulue et ensuite cliquez sur « *OK* ».

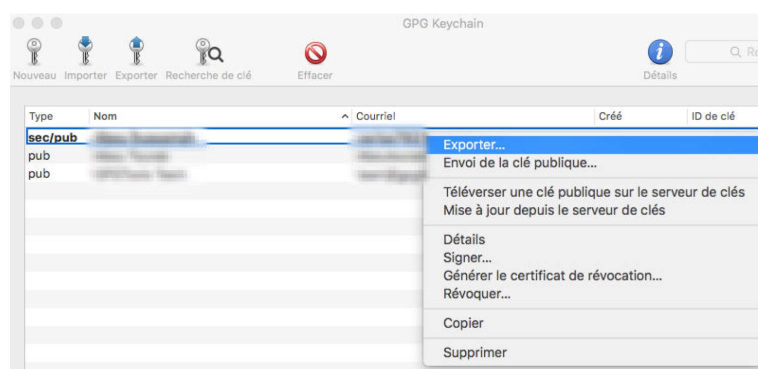


Vous avez alors maintenant votre message en version cryptée via la clef publique de la personne. Il ne vous reste plus qu'à l'envoyer par **E-mail**, ou un autre moyen de communication, pour qu'il le décrypte avec son propre code. (L'exemple ci-dessous est aussi un exemple fictif, non réel).



b) <u>Recevoir un message crypté :</u>

Vous devez fournir votre **clef publique** à la personne pour qu'elle crypte son message avec, comme vu dans le sous chapitre (**a**). Ouvrez « *GPG Keychain* », faites un clic droit sur votre **clef privée** et ensuite sélectionnez « *exporter* », enregistrez ensuite là où vous souhaitez et envoyez votre **clef publique** pour que la personne puisse la mettre dans sa liste.



Prenons maintenant l'exemple où vous venez de recevoir un message crypté, vu comme la dernière photo plus haut, pour le décrypter, rien de plus facile, sélectionnez le texte dans un éditeur de texte, et cliquez sur *Cmd* + *Shift* + *D*. Une fenêtre va alors s'ouvrir et vous invite à rentrer votre mot de passe choisi lors de la création de votre clef tout au début du tutoriel. Une fois le mot de passe rentré, votre message apparaît en mode décrypté.

Note : Si vous ne souhaitez pas ou ne pouvez pas faire les raccourcis clavier comme vu en haut du tutoriel pour Crypter/Décrypter, vous pouvez aussi faire un clic droit sur les messages et sélectionner « *services* » et vous aurez la liste des actions possibles.

Toutes les Louanges sont à Allah, Seul.

Nous demandons à Allah qu'Il préserve tous les frères et sœurs, et qu'Il aveugle les tawâghît et tous ses ennemis.